RACHELE R. BYRD (190634)
byrd@whafh.com
BRITTANY N. DEJONG (258766)
dejong@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599

MATTHEW M. GUINEY (*pro hac vice forthcoming*)
guiney@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
270 Madison Avenue
New York, NY 10016
Telephone: 212/545-4600
Facsimile: 212/545-4677

Attorneys for Plaintiffs

[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

KRISTA GILL and DOUG SUMERFIELD, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

HANNA ANDERSSON, LLC and SALESFORCE.COM, INC.

Defendants.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Krista Gill ("Gill") and Doug Sumerfield ("Sumerfield") (collectively, "Plaintiffs"), individually and on behalf of all other similarly situated individuals, hereby allege upon personal knowledge of the facts respectively pertaining to their own actions, and upon information and belief as to all other matters, by and through their undersigned counsel, and bring this Class Action Complaint against defendants Hanna Andersson, LLC ("Hanna Andersson") and Salesforce.com, Inc. ("Salesforce" and, collectively, "Defendants").

NATURE OF ACTION

1. Plaintiffs assert this class action against Defendants for their failure to exercise reasonable care in securing and safeguarding their customers' sensitive personal information ("SPI"), including customer names, payment card numbers, payment card expiration dates, and payment card security codes.

2. On January 15, 2020, Hanna Andersson sent letters to customers and states attorneys general stating that it "had obtained evidence that an unauthorized third party had accessed information entered on Hanna Andersson's website concerning purchases made between September 16 and November 11, 2019" (the "Data Breach").[1] Attempting to avoid the spotlight, Hanna Andersson sent this letter directly to customers and state law enforcement without making a public press release. News soon got out, however.

3. This type of customer payment data breach, called a Magecart attack, was simply the most recent in a long line of similar attacks on e-commerce platforms. The Hanna Andersson attack was no less than the second successful recent Magecart attack upon a platform that was part of Salesforce's Commerce Cloud Unit, its commercial hosting service.[2]

4. More broadly, Magecart attacks on online platforms have become very popular in the past few years. For example, Salesforce customer Macy's faced a similar Magecart attack

[1] https://www.documentcloud.org/documents/6662592-Hanna-Andersson-Notice-of-Data-Breach-to-Consumers.html (last visited Mar. 2, 2020).

[2] *See US Retailer Hanna Andersson Hacked to Steal Credit Cards*, BLEEPING COMPUTER, https://www.bleepingcomputer.com/news/security/us-retailer-hanna-andersson-hacked-to-steal-credit-cards/ (last visited Mar. 2, 2020).

last October where hackers successfully stole payment card information from its website for a week.[3]

5. Defendants could have prevented this Data Breach. Magecart attacks on e-ecommerce platforms are among the most popular types of attacks by hackers today. While many retailers, restaurant chains, and other companies have responded to data breaches by adopting technology that helps make transactions more secure, Defendants did not.

6. The Data Breach was the result of Defendants' inadequate approach to data security and protection of SPI that it collected during the course of its business. The deficiencies in Defendants' data security were so significant that the malware installed by hackers remained undetected and intact in Defendants' systems for approximately two months.

7. Defendants disregarded the rights of Plaintiffs and the Class by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard SPI, failing to take available steps to prevent the Data Breach, failing to monitor and timely detect the Data Breach, and failing to provide Plaintiffs and the Class prompt and accurate notice of the Data Breach.

8. As a result of Defendants' Data Breach, Plaintiffs' and Class members' SPI has been exposed to criminals for misuse and have, in fact, been misused. The injuries Plaintiffs and the Class suffered as a direct result of the Data Breach include:

a. unauthorized charges on debit and credit card accounts;

b. theft of personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts;

[3] *Macy's Hit by Magecart Card-Skimming Attack*, CISO MAG (Nov. 20, 2019), https://www.cisomag.com/macys-hit-by-magecart-card-skimming-attack/; *see also Macy's moves its mission-critical commerce app to Heroku*, SALESFORCE, https://www.salesforce.com/products/platform/app-gallery/macys/ (last visited Mar. 3, 2020).

d. damages arising from the inability to use debit or credit card accounts because accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the Data Breach, including but not limited to foregoing cash back rewards;

e. damages arising from the inability to withdraw or otherwise access funds because accounts were suspended, restricted, or otherwise rendered unusable as a result of the Data Breach, including, but not limited to, missed bill and loan payments, late-payment charges, and lowered credit scores and other adverse impacts on credit;

f. costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, lost productivity and opportunity(ies), time taken from the enjoyment of one's life, and the inconvenience, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury resulting from the potential fraud and identity theft posed by SPI being exposed for theft and sale on the dark web;

h. costs of products purchased at Defendants' website during the period of the Data Breach because Plaintiffs and the Class would not have purchased products from Defendants' website had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard SPI;

i. damages to and diminution in value of SPI entrusted to Defendants for the sole purpose of purchasing products and services from Defendants; and

j. the loss of Plaintiffs' and Class members' privacy.

9. The injuries Plaintiffs and the Class suffered were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for SPI.

10. Plaintiffs and the Class retain a significant interest in ensuring that their SPI, which remains in Defendants' possession, is protected from further breaches, and seek to remedy the harms suffered as a result of the Data Breach for themselves and on behalf of similarly situated consumers whose SPI was stolen.

11. Plaintiffs, individually and on behalf of similarly situated consumers, seek to recover damages, equitable relief, including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

PARTIES

12. Plaintiffs Krista Gill and Doug Sumerfield are natural persons and a married couple residing in Alexandria, Virginia.

13. Defendant Hanna Andersson, LLC is a Delaware corporation with its principal place of business at 608 NE 19th Ave., Portland, Oregon 97232. It is wholly-owned by L Catterton, a private equity company.

14. Defendant Salesforce.com, Inc. is a Delaware corporation with its principal place of business at 415 Mission St., San Francisco, California 94105.

JURISDICTION AND VENUE

15. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties to this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class.[4]

16. This Court has personal jurisdiction over Defendant Salesforce because its principal place of business is in the Northern District of California and Salesforce is authorized to and regularly conducts business in the Northern District of California.

[4] A letter sent to the North Dakota Attorney General by counsel for Hanna Andersson noted that there were 374 residents of North Dakota alone affected by the Data Breach.

17. This Court has personal jurisdiction over Defendant Hanna Andersson because it is authorized to do business and regularly conducts business in the Northern District of California. Hanna Andersson has no fewer than five physical stores in the Northern District of California and, on information and belief, Class members who were affected by the Data Breach placed orders from locations within the Northern District of California.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendants are corporations, Salesforce's principal place of business is within this District, and a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

A. Plaintiffs' Transactions

19. On or around September 26, 2019, Plaintiffs made an online purchase from hannaandersson.com.

20. On or around December 13, 2019, Plaintiffs were alerted by their bank to fraudulent activity on their credit card account, and their account was suspended until new cards could be issued to them, approximately five days later. For those five days, Plaintiffs were without the ability to use their joint credit card.

21. Plaintiffs' joint credit card that was compromised in the Data Breach is connected to a rewards program. While awaiting a replacement card following the Data Breach and fraudulent charges, Plaintiffs had to use alternative methods of payment and, thus, lost the opportunity to accrue rewards during that time.

22. After this occurred, Plaintiffs received notice on or about January 20, 2020 by mail from Hanna Andersson regarding the Data Breach.

23. Additionally, Plaintiff Krista Gill previously received data monitoring as part of a class action settlement from the Office of Personnel Management from MyIDCare services. This is the ***same*** data monitoring vendor whose services are offered by Hanna Andersson following the Data Breach. MyIDCare's monitoring was inadequate to prevent the Hanna Andersson Data Breach from causing damage to Plaintiffs, and is inadequate to address the Data Breach at the heart of this complaint.

24. Consequently, Plaintiffs lost time dealing with the issues related to the Data Breach in cancelling their credit card and in communicating with their financial institution.

25. Plaintiffs are not aware of any other relevant data breaches that could have resulted in the theft of their credit card information.

26. Plaintiffs suffered actual injury and damages in paying money to, and purchasing products from, Defendants' website during the Data Breach, expenditures which they would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' SPI from theft.

27. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their SPI—a form of intangible property that Plaintiffs entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

28. Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and have concerns for the loss of their privacy.

29. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their SPI being placed in the hands of criminals.

30. Plaintiffs have a continuing interest in ensuring their SPI, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

B. Hanna Andersson's Online Platform

31. Hanna Andersson is a retail corporation wholly owned by private equity company L Catterton. Hanna Andersson has at least 60 retail locations in the United States and a highly successful online retail presence.

32. Hanna Andersson produces and sells clothing and related products, mostly for children and infants, that are marketed as high-end. Hanna Andersson sells these products both in retail stores and online at hannaandersson.com.

33. Hanna Andersson's website states:

> The security of your personal information is very important to Hanna, and we have implemented measures to protect your information. Our website is PCI DSS compliant and uses SSL/TLS (Secure Sockets Layer) technology to encrypt your order information, such as your name, address, and credit card number, during data transmission. We use a third-party payment processor, which is also PCI DSS compliant.
>
> Our customer service center and stores also operate over a private, secure network.
>
> We follow generally accepted industry standards to protect the personal information submitted to us, both during transmission and once we receive it.[5]

34. Salesforce is a cloud-based software company that offers customer relationship management services to corporations, such as Hanna Andersson, that allow its clients to interact with customers, such as through online sales platforms, such as hannaandersson.com.

35. These online platforms, including hannaandersson.com, allow (among other things) for customers to make purchases of their clients' products through the use of payment cards. As part of the sales transactions, these platforms must collect highly sensitive SPI and personally identifiable information ("PII"), including payment card numbers, expiration dates, CVV codes, names, and billing and shipping addresses, as well as (potentially) email addresses and telephone numbers.

36. Platforms that allow this are marketed by Salesforce as the "Platform as a Service" ("PaaS") model.[6]

37. Salesforce says of its PaaS products, "(PaaS) is a proven model for running applications without the hassle of maintaining on-premises hardware and software infrastructure at your company. Enterprises of all sizes have adopted PaaS solutions like Salesforce for simplicity, scalability, and reliability. PaaS applications also have the latest features without the pain of constant upgrades."[7]

---

[5] *Privacy Statement*, HANNA ANDERSSON, https://www.hannaandersson.com/security-and-privacy.html (last visited Mar. 2, 2020).

[6] *See What is PaaS?*, SALESFORCE, https://www.salesforce.com/paas/overview/# (last visited Mar. 2, 2020).

[7] *Id.*

38. Further, Salesforce prominently markets its PaaS products as "**Secure** — Information is not vulnerable to a flood, fire, natural disaster, or hardware failure in one location. Security protocols and infrastructure are constantly analyzed and updated to address new threats."[8]

C. The Data Breach

39. A letter sent by Perkins Coie to the North Dakota Attorney General stated that Hanna Andersson was informed of the Data Breach on December 5, 2019 by "law enforcement" and that "credit cards used on its website were available for purchase on a dark web site."[9]

40. The letter further noted:

> The investigation has confirmed that Hanna Andersson's third-party ecommerce platform, Salesforce Commerce Cloud, was infected with malware that may have scraped information entered by customers into the platform during the purchase process. The earliest potential date of compromise identified by forensic investigators is September 16, 2019, and the malware was removed on November 11, 2019.

41. The letter further noted that physical letters were being mailed to customers believed to be affected by the breach and would be sent out beginning January 15, 2020.

42. The type of attack faced by Hanna Andersson and Salesforce is known as a "Magecart" attack, which has become very prevalent in recent years.[10]

43. "Magecart" is a consortium of hacker groups known from placing malware into online shopping cart systems in order to steal payment card information. As CSO Online stated,

---

[8] *What is Cloud Computing?*, SALESFORCE, https://www.salesforce.com/products/platform/best-practices/cloud-computing/?d=70130000000i88b (last visited Mar. 1, 2020).

[9] https://attorneygeneral.nd.gov/sites/ag/files/documents/DataBreach/2020-01-15-HannaAndersson.pdf (last visited Mar. 2, 2020).

[10] *See Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, THREATPOST, https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last visited Mar. 2, 2020).

"Almost all ecommerce sites that use shopping carts don't properly vet the code that is used with these third-party pieces — a recipe for a ready-made hack."[11]

44. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the SPI collected, maintained, and stored in the system's servers is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

45. Such malware can go undetected for a long period of time, especially if industry best practices are not routinely used.

46. SPI is a valuable commodity because it contains not only payment card numbers, but also PII. A "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal, private information on multiple underground Internet websites. SPI is valuable to identity thieves because they can it—including PII—to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, and credit cards.

47. Legitimate organizations and the criminal underground alike recognize the value of SPI and PII contained in a merchant's data systems, otherwise the latter would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . [n]ot only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing SPI and PII] from 38 million users."[12]

48. Professionals tasked with trying to stop fraud and other misuse know that SPI and PII have real monetary value in part because criminals continue their efforts to obtain this data.[13]

---

[11] *What is Magecart? How this hacker group steals payment card data*, CSO ONLINE, https://www.csoonline.com/article/3400381/what-is-magecart-how-this-hacker-group-steals-payment-card-data.html (last visited Mar. 2, 2020).

[12] *Verizon 2014 PCI Compliance Report* at 54, https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf.

[13] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, CIO MAGAZINE (Sept. 28, 2014), http://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html.

In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. However, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,579 data breaches in 2017, which represents a 44.7 percent increase over the record high figures reported for 2016.[14]

49. Consumers' SPI and PII remains valuable to identity criminals, as evidenced by the prices they will pay through black-market sources, or what is often called the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, a complete set of bank account credentials can fetch a thousand dollars or more (depending on the associated credit score or balance available to criminals).[15] Experian reports that a stolen credit or debit card number can sell for $5–110 on the dark web. [16]

50. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding SPI and PII, and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its customers as a result of a breach.

51. Defendants were, or should have been, fully aware of the significant volume of daily credit and debit card transactions on hannaandersson.com and, thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

52. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of SPI and PII in the hands of other third parties, such as retailers and restaurant chains, Defendants' approach to maintaining the privacy and security

---

[14] *2017 Annual Data Breach Year-End Review,* IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/2017-data-breaches (last visited Mar. 2, 2020).

[15] *Here's how much thieves make by selling your personal data online,* BUSINESS INSIDER (May 27, 2015), http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5.

[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

of Plaintiffs' and Class members' SPI and PII was lackadaisical, cavalier, reckless, or, at the very least, negligent.

D. The Data Breach Caused Harm and Will Result in Additional Fraud

53. Without detailed disclosures to Defendants' customers, Plaintiffs and Class members were unknowingly and unwittingly left exposed to continued misuse and ongoing risk of misuse of their SPI and PII without being able to take necessary precautions to prevent imminent harm.

54. Plaintiffs have already experienced fraud and loss of use of their payment card as a result of the breach.

55. Prior to the Data Breach, Plaintiffs routinely reviewed their credit report for unusual activity and had not received any indication that their credit card had been breached or otherwise compromised.

56. Plaintiffs never transmit unencrypted SPI or PII over the internet or any other unsecured source.

57. Plaintiffs store any and all documents containing their SPI and PII in a safe and secure location, and destroy/shred any documents they receive in the mail that contain any of their SPI or PII, or that may contain any information that could otherwise be used to compromise their credit cards, financial accounts, or steal their identities.

58. Thus, given that before the Data Breach, Plaintiffs' credit card had not experienced any prior form of breach or compromise and Plaintiffs undertook substantial efforts to protect their financial information—including SPI and PII—Defendants' Data Breach is the source of Plaintiffs' damages and injuries described in this Complaint.

59. But for the Data Breach, Plaintiffs' credit card would not have been breached or compromised and their damages would not have occurred.

60. The ramifications of Defendants' failure to keep Plaintiffs' and Class members' data secure are severe and far reaching.

61. Additionally, Hanna Andersson has offered a one-year subscription to MyIDCare identity protection services, offered by ID Experts.[17] However, MyIDCare is ***the same service used by the Office of Personnel Management*** as a result of that data breach.[18] MyIDCare did not stop Plaintiffs' data from being stolen as part of this Data Breach, and will not be sufficient to protect Defendants' consumers identities going forward.

62. Consumer victims of data breaches are more likely to become victims of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.[19]

63. The Electronic Code of Federal Regulations defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[21]

64. SPI and PII are valuable commodities to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have SPI and PII, "they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[22]

---

[17] *See* https://ago.vermont.gov/wp-content/uploads/2020/01/2020-01-14-Hanna-Andersson-Notice-of-Data-Breach-to-Consumers.pdf (last visited Mar. 2, 2020).

[18] *See Victims enrolled in OPM's identity protection service are covered through June, agency says*, FEDERAL NEWS NETWORK, https://federalnewsnetwork.com/opm-cyber-breach/2018/11/victims-enrolled-in-opms-identity-protection-service-are-covered-through-june-agency-says/ (last visited Mar. 2, 2020).

[19] 2014 LexisNexis True Cost of Fraud Study (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

[20] 17 C.F.R § 248.201 (2013).

[21] *Id.*

[22] *Warning Signs of Identity Theft*, FEDERAL TRADE COMMISSION, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Mar. 2, 2020).

65. Identity thieves can use SPI and PII, such as that of Plaintiffs and Class members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

66. Analysis of a 2016 survey of 5,028 consumers found, "The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[23]

67. As a result of Defendants' delay in notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class members has been driven even higher.

68. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the six years preceding 2016.[24]

69. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[25]

---

[23] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, JAVELIN (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

[24] *See 2016 Identity Fraud: Fraud Hits an Inflection Point*, JAVELIN (Feb. 2, 2016), https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point.

[25] Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEP'T OF JUSTICE (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

70. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly US $215 per cardholder incurring these charges,[26] some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

71. Plaintiffs and the Class now face a real, immediate, and continuing risk of identity theft and fraudulent payment card charges resulting from Defendants' actions and negligence, as well as the expense in forgoing use of cancelled cards and the time and effort expended in changing credit card numbers.

72. The processes of discovering and dealing with the repercussions of identity theft and fraudulent payments are time consuming and difficult. The Bureau of Justice Statistics reports that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."[27]

73. The victims here—Plaintiffs and the Class—are no different, as they are faced with an arduous path to secure their SPI in response to Defendants' negligence. Plaintiffs and the Class either have or must take at least the following steps to attempt to prevent further misuse of their SPI:

a. Review and monitor credit card statements for any unusual or unknown charges;

b. Contact their financial institution to determine if there is any suspicious activity on their accounts;

c. Change their account information; and

[26] Hadley Malcom, *Consumers rack up $14.3 billion in 'gray' charges*, USA TODAY (July 25, 2013), https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/.

[27] Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE, (Dec. 2013), http://www.bjs.gov/content/pub/pdf/vit12.pdf.

d. Periodically monitor their credit bureau reports for any unusual activity and check for accuracy.

74. Additionally, there is commonly lag time between when harm occurs and when it is discovered and also between when SPI is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[28]

75. There is a very strong probability that those impacted by Defendants' failure to secure their SPI and PII could be at risk of fraud and identity theft for extended periods of time.

76. Thus, Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, regardless of whether such charges are ultimately reimbursed by banks and credit card companies.

E. Plaintiffs and Class Members Suffered Damages

77. Plaintiffs' and Class members' SPI and PII is private and sensitive in nature and was left inadequately protected by Defendants. Defendants did not obtain Plaintiffs' and Class members' consent to disclose their SPI and PII to any other person as required by applicable law and industry standards.

78. The Data Breach was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiffs' and Class members' SPI and PII from unauthorized

[28] *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown,* U.S. GOV'T ACCOUNTABILITY OFFICE (June 2007), https://www.gao.gov/new.items/d07737.pdf.

access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' SPI and PII to protect against reasonably foreseeable threats to the security or integrity of such information.

79. Defendants had the resources to prevent a breach. Upon information and belief, Defendants made significant expenditures to market its products, but neglected to adequately invest in data security, despite the growing number of, and several years of well-publicized, data breaches.

80. Had Defendants remedied the deficiencies in its online sales platform system, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Defendants would have prevented intrusion into their online sales platform system and, ultimately, the theft of their customers' confidential SPI and PII.

81. As a result of Defendants' wrongful actions, inaction, negligent security practices, and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing and increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands, such as work and family, and instead spend it on efforts to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

82. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class members' SPI and PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and misused via the sale of Plaintiffs' and Class members' information on the Internet's black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their SPI

f. the improper disclosure of their PII;

g. loss of privacy;

h. money paid for goods purchased at Defendants' website during the period of the Data Breach in that Plaintiffs and Class members would not have shopped at hannaandersson.com, or at least would not have used their payment cards for purchases, had Defendants disclosed that they lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information and had Defendants provided timely and accurate notice of the Data Breach;

i. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

j. ascertainable losses in the form of deprivation of the value of their SPI and PII, for which there is a well-established national and international market;

k. ascertainable losses in the form of the loss of cash-back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

l. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

m. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

83. While Plaintiffs' and Class members' SPI and PII have been stolen, Defendants continue to hold consumers' SPI and PII, including that of Plaintiffs and Class members. Particularly because Defendants have demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and Class members have an undeniable interest in ensuring that their SPI and PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

84. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and (c)(4), seeking damages and equitable relief on behalf of the following nationwide Class for which Plaintiffs seek certification:

> All persons residing in the United States who made a credit or debit card purchase on hannaandersson.com during the period of the Data Breach (the "Nationwide Class").

85. Excluded from the Class are Defendants; any parent, affiliate, or subsidiary of Defendants; any entity in which Defendants have a controlling interest; any of Defendants' officers or directors; and any successor or assign of Defendants. Also excluded are any Judge or court personnel assigned to this case and members of their immediate families.

86. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

87. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the Class is so numerous that joinder of all members is impracticable. While Plaintiffs do not know the exact

number of Class members, Plaintiffs believe there are at least hundreds of thousands. As stated *supra*, Hanna Andersson provided notice to all Class members it was aware of through notice by mail in mid-January 2020. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media, and/or published notice.

88. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirements, common questions of law and fact exist as to all members of the Class and predominate over any questions affecting individual Class members. Such questions of law and fact common to the Class include, but are not limited to:

a. Whether Defendants had a duty to adequately protect SPI;

b. Whether Defendants had a duty to adequately protect PII;

c. Whether Defendants knew or should have known of the susceptibility of its online sales platform to a data breach;

d. Whether Defendants' security measures to protect its website were reasonable in light of FTC data security recommendations and best practices recommended by data security experts;

e. Whether Defendants engaged in the wrongful conduct alleged herein;

f. Whether Defendants were negligent in failing to implement reasonable and adequate security procedures and practices;

g. Whether Defendants' failure to implement adequate data security measures allowed the breach of its online sales platform to occur;

h. Whether Defendants' conduct constituted unfair or deceptive trade practices;

i. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of the website, resulting in the loss of Plaintiffs' and Class members' SPI and PII ;

j. Whether Plaintiffs and Class members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect the website; and

k. Whether Plaintiffs and Class members are entitled to relief, including equitable relief.

89. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with rule 23(a)(3), Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs are consumers who used their payment cards on the Hanna Andersson website and had their cards compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class members, and Plaintiffs seek relief consistent with the relief of the Class members.

90. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendants to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class members. Plaintiffs' counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other members of the Class. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other members of the Class.

91. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and, thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action

device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

92. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

93. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their SPI and PII;

c. Whether Defendants' security measures to protect the website were reasonable in light of FTC data security recommendations, and other best practices recommended by data security experts;

d. Whether Defendants' failure to adequately protect their website amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard Plaintiffs' and the Class members' SPI and PII; and

f. Whether adherence to FTC data security recommendations and measures recommended by data security experts would have reasonably prevented the Data Breach.

94. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to information regarding the Data Breach, including the time period of the Data Breach and which customers were potentially affected. Using this information, Class members can be identified and their contact information ascertained for the purpose of providing notice to the Class.

FIRST CLAIM FOR RELIEF
Negligence
(On behalf of Plaintiffs and the Class)

95. Plaintiffs restate and reallege paragraphs 1 through 94 as if fully set forth herein.

96. Defendants solicited and took possession of Plaintiffs' and the Class members' SPI and PII, and Defendants had a duty to exercise reasonable care in securing that information from unauthorized access or disclosure. Defendants also had a duty to timely notify Plaintiffs and the Class that their SPI and PII had been or may have been stolen.

97. Upon accepting and storing Plaintiffs' and Class members' SPI and PII in its computer systems and on its networks, Defendants undertook and owed a duty of care to Plaintiffs and Class members to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' SPI and PII and to use commercially-reasonable methods to do so. Defendants knew that the SPI and PII was private and confidential, and should be protected as private and confidential.

98. Defendants owed a duty of care not to subject Plaintiffs and Class members, along with their SPI and PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

99. Defendants owed a duty of care to Plaintiffs and Class members to quickly detect a data breach and to timely act on warnings about data breaches.

100. Defendants' duties arose from their relationship to Plaintiffs and Class members and from industry custom.

101. Defendants, through their actions and/or failures to act, unlawfully breached duties to Plaintiffs and Class members by failing to implement standard industry protocols and to exercise reasonable care to secure and keep private the SPI entrusted to it.

102. Defendants, through their actions and/or failures to act, allowed unmonitored and unrestricted access to unsecured SPI and PII.

103. Defendants, through their actions and/or failures to act, failed to provide adequate supervision and oversight of the SPI and PII with which they were entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third

parties to gather Plaintiffs' and Class members' SPI and PII, misuse that SPI and PII, and intentionally disclose it to unauthorized third parties without consent.

104. Defendants knew, or should have known, the risks inherent in collecting and storing SPI and PII, the vulnerabilities of online sales platform systems, and the importance of adequate security. Defendants were aware of numerous, well-publicized data breaches.

105. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' SPI and PII.

106. Due to Defendants' knowledge that a breach of their systems would damage their customers, including Plaintiffs and Class members, Defendants had a duty to adequately protect their data systems and the SPI and PII contained thereon.

107. Defendants had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Defendants with their SPI and PII was predicated on the understanding that Defendants would take adequate security precautions to safeguard that information. Moreover, only Defendants had the ability to protect their systems and the SPI and PII stored on those systems from attack.

108. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their SPI and PII. Defendants' misconduct included failing to: (1) secure the website, despite knowing its vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

109. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiffs' and Class members' SPI and PII, and promptly notify them about the Data Breach.

110. Defendants breached its duties to Plaintiffs and Class members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' SPI and PII;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class members' SPI and PII before and after learning of the Data Breach;

d. by failing to comply with industry standard data security measures during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiffs' and Class members' SPI and PII had or had likely been improperly acquired or accessed.

111. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and their failure to protect Plaintiffs' and Class members' SPI and PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' SPI and PII while it was within Defendants' possession or control.

112. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of Plaintiffs' and Class members' SPI and PII, so that Plaintiffs and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their SPI and PII.

113. Defendants breached their duty to notify Plaintiffs and Class Members of the unauthorized access to their SPI and PII by waiting to notify Plaintiffs and Class members, and then by failing to provide Plaintiffs and Class members with sufficient information regarding the breach.

114. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect Plaintiffs' and Class members' SPI and PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect

and secure Plaintiffs' and Class members' SPI and PII while it was within Defendants' possession or control.

115. Further, through their failure to provide timely and clear notification of the Data Breach to consumers, Defendants prevented Plaintiffs and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

116. Upon information and belief, Defendants improperly and inadequately safeguarded Plaintiffs' and Class members' SPI and PII in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendants' failure to take proper security measures to protect sensitive SPI and PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class members' SPI and PII.

117. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the SPI and PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class members' SPI and PII; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive SPI and PII had been compromised.

118. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their SPI and PII as described in this Complaint

119. Defendants' failure to exercise reasonable care in safeguarding SPI and PII by adopting appropriate security measures, including proper encryption storage techniques, was the direct and proximate cause of Plaintiffs' and Class members' SPI and PII being accessed and stolen through the data breach.

120. Defendants breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' SPI and PII.

121. As a result of Defendants' breach of duties, Plaintiffs and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their

debit or credit cards or on cards that were fraudulently obtained through the use of their SPI and PII; damages arising from Plaintiffs' and Class members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports; and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

SECOND CLAIM FOR RELIEF
Declaratory Judgment
(On behalf of Plaintiffs and the Class)

122. Plaintiffs restate and reallege paragraphs 1 through 94 as if fully set forth herein.

123. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Defendants to provide adequate security for the SPI and PII it collected from their payment card transactions. As previously alleged, Defendants owe duties of care to Plaintiffs and Class members that require them to adequately secure SPI and PII.

124. Defendants still possess SPI and PII pertaining to Plaintiffs and Class members.

125. Defendants have not announced or otherwise notified Plaintiffs and Class members that their SPI and PII are sufficiently protected.

126. Accordingly, Defendants have not satisfied their contractual obligations and legal duties to Plaintiffs and Class members. In fact, now that Defendants' lax approach towards data security has become public, the SPI and PII in its possession is more vulnerable than before.

127. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

128. Plaintiffs, therefore, seek a declaration that: (a) Defendants' existing data security measures do not comply with their contractual obligations and duties of care; and (b) in order to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems are compromised, hackers cannot gain access to other portions of Defendants' systems;

e. purging, deleting, and destroying SPI and PII not necessary for their provision of services in a reasonably secure manner;

f. conducting regular database scans and security checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants' customers should take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, respectfully seek from the Court the following relief:

a. Certification of the Class as requested herein;

b. Appointment of Plaintiffs as Class representatives and their undersigned counsel as Class counsel;

c. An order awarding Plaintiffs and members of the proposed Class damages;

d. An order awarding Plaintiffs and members of the proposed Class equitable, injunctive and declaratory relief, including the enjoining of Defendants' insufficient data protection practices at issue herein and Defendants' continuation of their unlawful business practices as alleged herein;

e. An order declaring that Defendants' acts and practices with respect to the safekeeping of SPI and PII are negligent;

f. An order awarding Plaintiffs and members of the proposed Class pre-judgment and post-judgment interest as permitted by law;

g. An order awarding Plaintiffs and members of the proposed Class reasonable attorney fees and costs of suit, including expert witness fees; and

h. An order awarding Plaintiffs and members of the proposed Class any further relief the Court deems proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and the Class of all others similarly situated, hereby demand a trial by jury on all issues so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

DATED: March 3, 2020

Respectfully submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

/s/ Rachele R. Byrd
RACHELE R. BYRD

RACHELE R. BYRD
byrd@whafh.com
BRITTANY N. DEJONG
dejong@whafh.com
Symphony Towers
750 B Street, Suite 1820
San Diego, California
Telephone: 619/239-4599
Facsimile: 619/234-4599

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
MATTHEW M. GUINEY
guiney@whafh.com
(*pro hac vice forthcoming*)
270 Madison Avenue
New York, New York 10016
Telephone: 212/545-4600
Facsimile: 212/545-4653

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
CARL MALMSTROM
malmstrom@whafh.com
(*pro hac vice forthcoming*)
111 W. Jackson St., Suite 1700
Chicago, IL 60604
Telephone: 312/984-0000
Facsimile: 212/545-4653

Attorneys for Plaintiffs

26299v2